DECLARATION

I, Elizabeth Nawalaniec, a Special Agent with the Federal Bureau of Investigation, state under the penalty of perjury, pursuant to Title 28, United States Code, Section 1746, that the following is true and correct.

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since October 2023. I am currently assigned to the FBI's Charlotte Field Office, Greensboro Resident Agency. In this capacity, I am charged with investigating possible violations of federal criminal law. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on criminal cases. At the start of my employment, I received training on how to conduct criminal investigations at the FBI Academy in Quantico, Virginia. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants, seizures, and the identification and collection of evidence. From my training and experience, I have also become familiar with the techniques and methods used by criminal enterprises to evade law enforcement while conducting criminal activity, to include myriad ways to launder proceeds from illicit activity or forms of communication utilized to avoid law enforcement detection. In addition, I have worked with and consulted numerous agents and law enforcement officers who have conducted complex criminal enterprise investigations throughout the United States and beyond. Prior to becoming a Special Agent, I was employed by the FBI in multiple positions in FBI field offices and headquarters for over six years. In my prior roles with the FBI, I assisted with a variety of national security matters and criminal investigations.

EXHIBIT
A

2. This declaration is in support of a Verified Complaint of Forfeiture for the defendant properties that are currently in the custody of the United States Marshals Service:

a. 242,406.102 USDT in funds from Tether Ltd. virtual currency address ending in F544 ("Subject Address 1");

b. 235,680.00 USDT in funds from Tether Ltd. virtual currency address ending in 5ad0 ("Subject Address 2");

c. 223,743,002 USDT in funds from Tether Ltd. virtual currency address ending in 48D4 ("Subject Address 3"); and

d. 220,000.00 USDT in funds from Tether Ltd. virtual currency address ending in 6cfC ("Subject Address 4").

(collectively the "Subject Addresses").

3. The facts and information contained in this Declaration come from my personal observations, my training and experience, and information from other agents, witnesses, and agencies. Because this Declaration is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation.

4. Based on the information in this Declaration, there is probable cause to believe that abovementioned properties were involved in transactions or attempted transactions in violation of Title 18, United States Code, Section 1956 and 1957 (Money Laundering), or are traceable to such properties, or constitute or were derived from

proceeds traceable to violations of Title 18, United States Code, Section 1343, and are therefore subject to forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(A) and (a)(1)(C).

BACKGROUND

5. Virtual currencies are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (*i.e.*, they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (*e.g.*, online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.

6. A virtual currency address is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received. A virtual currency address is associated with a virtual currency wallet. A virtual currency wallet

(*e.g.*, a hardware wallet, software wallet, or paper wallet) stores a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses can be controlled by one wallet. An unhosted wallet, also known as a self-hosted or non-custodial wallet, is a virtual currency wallet through which the user has complete control over storing and securing their private keys and virtual currency. Unhosted wallets do not require a third party's involvement (*e.g.*, a virtual currency exchange) to facilitate a transaction involving the wallet.

7. A public key is a cryptographic key that is uniquely associated with a person or entity and is designed to be made public. The public key is paired with, and derived from, a private (secret) key. However, knowing the public key does not reveal any information about the private key. In the blockchain and virtual currency context, a virtual currency address is the hashed value of a public key and acts as an identifier on a blockchain. A private key is a cryptographic key that is uniquely associated with an entity and not made public. In the blockchain and virtual currency context, virtual currency addresses are controlled using a unique corresponding private key, the equivalent of a password, which is needed to access the funds associated with the address. Only the holder of an address's private key can authorize a transfer of virtual currency from that address to another address.

8. A blockchain is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets,

including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin exists on the Bitcoin blockchain, while Ether (or "ETH") exists on the Ethereum network.

9. A transaction fee is a fee paid by the party sending virtual currency on a blockchain to reward miners and/or validators for verifying and validating transactions. Transaction fees vary by blockchain and can fluctuate based on factors such as blockchain network traffic and transaction sizes. Senders of virtual currency can increase the transaction fees that they pay to have their transactions confirmed faster by miners and/or validators. Transaction fees are generally paid in a blockchain's native token (*e.g.*, Bitcoin on the Bitcoin blockchain). On the Ethereum network, these transaction fees are called "gas fees." Gas fees are transaction costs paid in Ether ("ETH"), or its fraction, gwei. These fees serve as a form of remuneration for validators who maintain and secure the network. Gas fees fluctuate based on supply, demand, and network capacity, and may increase during periods of network congestion.

10. A virtual currency exchange ("VCE"), also called a cryptocurrency exchange, is a platform used to buy and sell virtual currencies. VCEs allow users to exchange their virtual currency for other virtual currencies or fiat currency, and vice versa.

Many VCEs also store their customers' virtual currency addresses in hosted wallets. VCEs can be centralized (*i.e.*, an entity or organization that facilitates virtual currency trading between parties on a large scale and often resembles traditional asset exchanges like the exchange of stocks) or decentralized (*i.e.*, a peer-to-peer marketplace where transactions occur directly between parties).

11. Decentralized Finance, or DeFi, is an umbrella term for peer-to-peer financial services on public blockchains, primarily the Ethereum network, that do not require traditional centralized financial intermediaries. DeFi platforms can offer a range of financial services involving digital assets, including the ability for users to lend, invest, earn interest, and exchange digital assets. DeFi platforms provide these services by using self-executing agreements written in code, known as "smart contracts," and these smart contracts are made accessible to users through decentralized applications (or "DApps").

12. Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, USDC and USDT are stablecoins pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives. Tether Limited ("Tether") is a company that manages the smart contracts and the treasury (*i.e.*, the funds held in reserve) for USDT tokens. Because Tether manages the smart contracts for USDT, it is able to blacklist some addresses containing USDT.

13. Law enforcement can trace transactions on blockchains to determine which virtual currency addresses are sending and receiving particular virtual currency. This analysis can be invaluable to criminal investigations for many reasons, including that it may enable law enforcement to uncover transactions involving illicit funds and to identify the person(s) behind those transactions. To conduct blockchain analysis, law enforcement officers use reputable, free open-source blockchain explorers, as well as commercial tools and services. These commercial tools are offered by different blockchain-analysis companies. Through numerous unrelated investigations, law enforcement has found the information associated with these tools to be reliable.

14. Cryptocurrency investment schemes (also known as "pig butchering") are schemes where criminal actors engage in social engineering, which allow the criminal actors to steal victims' funds through virtual currency payments and/or fraudulent investments. The phrase "pig butchering" is translated from the Chinese "shāzhūpán" and refers to a scam in which the victim is "fattened up prior to slaughter." Pig butchering scams typically involve four stages. First, a perpetrator will use a fictious identity and cold-contact a victim, often via text message or messaging application, social media, a dating application, or other communication platform. Oftentimes, the perpetrator will pretend to have contacted the wrong number but will continue communicating with the victim. Second, the perpetrator will establish a relationship and build trust with the victim by continuing to message over days, weeks, or months. Third, the scammer will concoct a narrative to induce the victim to send a series of payments in the form of virtual currency.

Common narratives include lucrative investment opportunities or emergencies necessitating funds. Many perpetrators will convince victims to use fraudulent websites or applications, controlled by scammers, to invest in virtual currency. Perpetrators coach victims through the investment process, show them fake profits, and encourage victims to invest more. In the fourth stage, perpetrators disengage victims once they have stolen their funds. In scenarios when victims stop sending more payments, the perpetrator cuts off all contact. In schemes involving fraudulent investment platforms, victims are told they need to pay a fee or tax when they attempt to withdraw their money. Victims are then unable to get their money back from the perpetrators, even if they pay the fake fees or taxes.

15. Based on data submitted to the FBI's Internet Crime Complaint Center ("IC3"), in 2023 alone, virtual currency investment schemes resulted in over thirty thousand complaints and over three billion dollars in losses.

16. The virtual currency ecosystem is used by criminals not only to receive victim money, but to launder it quickly, anonymously, and at scale. Like traditional money laundering, laundering money through cryptocurrency shares the same three stages of placement, layering, and integration, with different techniques applied within each:

- *Placement* – Criminals use non-custodial, or "private" wallets to initially receive victim funds. This is because such wallets are unattributable by blockchain analysis alone, are simple to create, and can accept large transaction amounts without additional scrutiny.

- *Layering* – Next, criminals will have victim funds transverse numerous private wallets, consolidate with other illegitimate and sometimes legitimate funds, and be subjected to other more cryptocurrency-specific processes to obfuscate both the origin of, and the ultimate destination for, the victim funds.
- *Integration* – Finally, by using a diffuse network of "brokers," who agree to exchange cryptocurrency for fiat using various means, criminals render their proceeds liquid and fully integrated with the legitimate financial system.

THE INVESTIGATION

17. An investigation by the FBI San Diego Field Office into cryptocurrency investment schemes identified J.M., a 59-year-old resident of Greensboro, North Carolina, as a potential victim. FBI alerted J.M. On June 19, 2024, J.M. reported that he suffered a loss of approximately $2.6 million due to a cryptocurrency investment scheme.

18. J.M. reported that, in or about early 2024, he met an individual who identified herself as "Emily CHAN" (CHAN) on an online dating platform. CHAN told J.M. she lived in Chicago, Illinois and worked for "Apparel Agency." After developing a relationship with J.M., CHAN shared information about how she made a significant amount of money investing through a special cryptocurrency offer. CHAN stated the

investment provided high returns and could be accessed through the DApp "saving.best" in the software wallet Trust Wallet.

19. In May 2024, CHAN convinced J.M. to invest in the special offer. Through communication on the messaging platform WhatsApp, CHAN instructed J.M. to transfer money from his bank accounts into accounts created on the cryptocurrency exchanges Kraken and Strike. CHAN then instructed J.M. to purchase two types of cryptocurrency, BTC (Bitcoin) and USDC, and to transfer these funds to his Trust Wallet unhosted wallet. CHAN helped J.M. set up a saving.best account and provided step-by-step instructions to connect his Trust Wallet to the saving.best platform to access the "investment opportunity." In the process of connecting his Trust Wallet to saving.best, J.M. was prompted to accept a token approval, which granted permission for another address to spend the entirety of the cryptocurrency in the wallet. The saving.best platform appeared to show J.M's "investment" receiving dividends daily, increasing the amount of USDC in the account. However, in reality, the funds were drained from the account. CHAN then convinced J.M. to invest with her in a "smart contract" that she had access to because she had a sister who worked at "Ethereum blockchain" and to merge his account with hers to further increase returns. According to the "contract," J.M. and CHAN together needed to invest $8 million.

20. Based on the above and my knowledge of virtual currency and cryptocurrency investment schemes, I believe saving.best to be a fraudulent platform.

21. After a period of time, J.M. was told the merged account was "locked" because the account balance exceeded $8 million. CHAN told J.M. to have the account

"unlocked," a new contract for $12 million was required. J.M. was told until the account reached $12 million, no funds could be withdrawn. CHAN continued to pressure J.M. to add funds to reach $12 million, but he had no additional funds to add. J.M. was never able to recover any of his funds.

22. On June 20, 2024, another victim filed an IC3 complaint regarding a cryptocurrency investment scheme involving saving.best. In similar fashion, this victim was encouraged and provided step-by-step instructions by a woman he met online to invest approximately $16,000 through a Trust Wallet which was then connected to saving.best. This victim believed his account to be receiving dividends daily but was also unable to withdrawal funds from the wallet.

TRACING OF VICTIM'S FUNDS

23. An FBI Forensic Accountant traced a portion of J.M.'s payments on the blockchain and identified a network of cryptocurrency addresses used to receive and launder J.M.'s payments. Three transactions, totaling 2,172,030 USDC (worth approximately $2,176,042 USD), were sent from J.M's Trust Wallet to two addresses that purportedly belonged to saving.best. Approximately 1,769,395 USDC of these funds were then moved through multiple intermediary wallets and finally deposited into a consolidation address. After the funds were received in the consolidation address, they were converted to USDT and a significant portion of the funds were deposited into the four

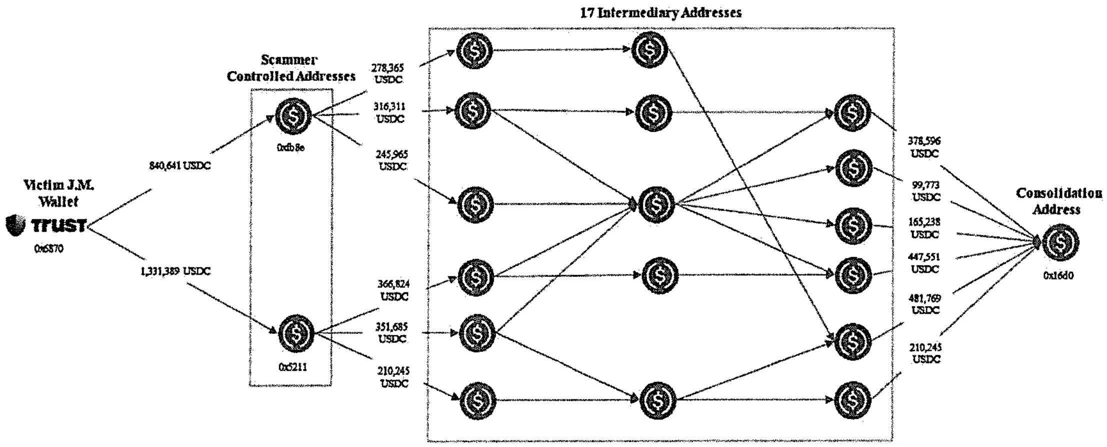
Subject Addresses. Approximately 870,155 USDT out of the total 921,829 USDT in the Subject Addresses can be traced back to J.M.

VICTIM FUNDS ARE SENT TO A CONSOLIDATION ADDRESS

24. In cryptocurrency investment schemes, after a victim sends funds to an address, the perpetrators usually move the funds to another address within minutes or hours of the victim's deposit. Frequently, the funds are then quickly moved into "consolidation addresses," which combine the funds sent by various victims and/or recombine stolen funds after they have been moved through various addresses.

25. On June 1, 2024, a payment from J.M.'s Trust Wallet, address 0x6870abd0e90168fbf3d2306cf33e64e540fabace (0x6870), in the amount of 1,331,389 USDC was sent in one transaction to an address purportedly controlled by saving.best, 0x5211fbfdc674035cacbf6e55a555cd22fc2adaff (0x5211). On June 7, 2024 and June 10, 2024, payments totaling 840,641 USDC were sent from J.M.'s Trust Wallet in two transactions to an address purportedly controlled by saving.best, 0xfb8ea633b635684c808ac6b1c7b3fa5bd9bf1a51 (0xfb8e). After receiving J.M.'s funds, addresses 0x5211 and 0xfb8e almost immediately sent corresponding payments to six intermediate addresses. These addresses continued to pass J.M's funds through additional intermediary addresses, and based on the last in-first out ("LIFO") accounting principle, which assumes the last, or most recent, incoming assets are the first expended or sent out, the FBI calculated approximately 1,769,395 USDC of J.M.'s funds ultimately ended up at consolidation address 0x16d09bda8c15123177f75a3c8fb53c5b2bbe2779 (0x16d0). The

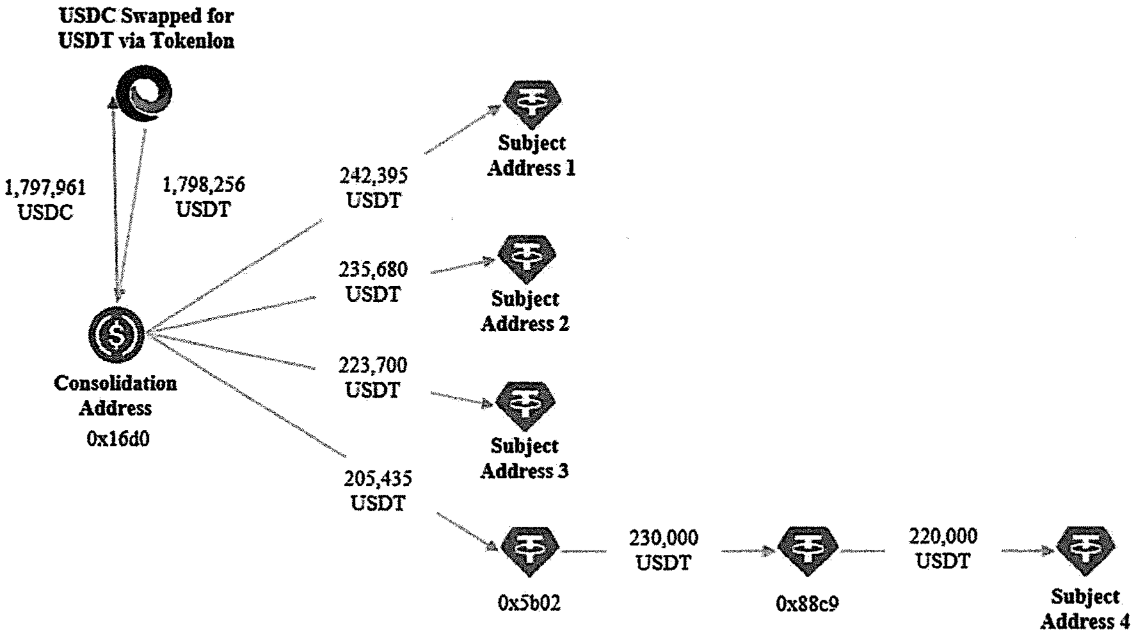
total amount of USDC sent to the consolidation address in the illustration below is approximately 13,777 higher than the amount traced back to J.M.'s funds because J.M.'s funds were commingled with other funds and then sent to the consolidation address. The flow of J.M.'s funds is illustrated below:



26. I know of no reason, economic or otherwise, for legitimate businesses or individuals to conduct virtual currency transfers in the above fashion. When transferring virtual currency, in this case USDC, on the Ethereum blockchain, each individual transfer costs money, a transaction fee. It is reasonable to assume that legitimate businesses and individuals would strive to minimize those fees by conducting transfers with as few transactions, or "hops," as possible.

LAUNDERING FUNDS FROM THE CONSOLIDATION ADDRESS TO THE SUBJECT ADDRESSES

27. The illustration below shows the movement of funds from the consolidation address to the four Subject Addresses. After J.M's funds were moved into the consolidation address on June 1, 2024 and June 11, 2024, the actors swapped 840,641 USDC for 840,665 USDT and 957,320 USDC for 957,592 USDT. These conversions or swaps were executed using the decentralized exchange Tokenlon. Based on the LIFO accounting principle, approximately 1,769,395 USDC or 98% of the total 1,797,961 USDC swapped for USDT through Tokenlon could be traced back to J.M.'s original payments.



28. Criminals will often swap or convert cryptocurrency assets that constitute the proceeds of unlawful activity to try to conceal or disguise the funds.

29. On June 11, 2024, after the USDC was swapped for USDT through Tokenlon, the consolidation address sent 242,395 USDT to Subject Address 1, then 235,680 USDT to Subject Address 2, and finally 223,700 USDT to Subject Address 3.

30. On June 1, 2024, after the USDC was swapped for USDT through Tokenlon, the consolidation address sent 205,435 USDT to cryptocurrency address 0x5b027d7cba939d6f4606743227a11ac07a5f09a9 (0x5b027). The next day, address 0x5b02 sent 230,000 USDT to cryptocurrency address 0x88c952df3ffb81ca9f8b747c085a17c25f1c928c (0x88c9). Finally, on June 15, 2024, address 0x88xc9 sent 220,000 USDT to Subject Address 4.

31. Approximately 870,155 USDT out of the 921,829 USDT in the subject addresses can be traced back to J.M.

32. On June 22, 2024, Tether voluntarily froze the Subject Addresses which, at the time, contained a total of 921,307 USDT. Subject Addresses 1, 2, 3, and 4 maintained the following balances as of December 2024:

Address	Balance
Subject Address 1	242,406 USDT
Subject Address 2	235,680 USDT
Subject Address 3	223,743 USDT
Subject Address 4	220,000 USDT
Total:	921,829 USDT

33. On December 18, 2024, I applied for a seizure warrant to seize All Funds from the Subject Addresses. After reviewing the probable cause affidavit, U.S. Magistrate Judge Joi Elizabeth Peake issued the seizure warrant (1:24MJ563).

34. On or about April 4, 2025, the virtual currency in the Subject Addresses described in paragraph 2 was "burned" (*i.e.*, destroyed) by Tether, and Tether reissued the equivalent amounts of USDT to a virtual currency wallet address controlled by the United States Marshals Service (USMS). The funds are currently being held pending forfeiture in the USMS-controlled wallet address.

CONCLUSION

35. Based on the foregoing, there is probable cause to believe the defendant properties were involved in a transaction or attempted transactions in violation of Title 18, United States Code, Sections 1956 or 1957, or are traceable to such properties, and are therefore subject to forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(A); and that the defendant properties constitute or were derived from proceeds traceable to violations of Title 18, United States Code, Section 1343, or a conspiracy to commit such offense, and are therefore subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C).

This the 19th day of May, 2025.

Elizabeth Nawalaniec
Special Agent
Federal Bureau of Investigation